UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/933,760	08/22/2001	Timothy C. Williams	P62141US1	6977

136 7590 12/17/2003

JACOBSON HOLMAN PLLC
400 SEVENTH STREET N.W.
SUITE 600
WASHINGTON, DC 20004

EXAMINER	
KIM, JUNG W	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 12/17/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/933,760	WILLIAMS, TIMOTHY C.	
	Examiner	Art Unit	
	Jung W Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *25-32,34-45 and 47-84* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *25-32,34-45 and 47-84* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 August 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☒ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 5 .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Claim Objections

Claim 36 is objected to because of the following informalities: The sentence of claim 36 is not grammatical. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 54, 66, 73, and 82 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claims 54, 66, 73, and 82, the phrase "such as" renders the claim indefinite because it is unclear whether the limitations following the phrase are part of the claimed invention. See MPEP § 2173.05(d).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 25-27, 31, 36-40, 44, 49-51, 53, 60-65, 69, 71, 72, 74, 76-79, 81, and 83 are rejected under 35 U.S.C. 102(b) as being anticipated by Boyle et al. U.S. Patent No. 5,577,209 (hereinafter Boyle). As per claim 25, Boyle discloses a secure network having a plurality of host computers accessible to users and connected to a network medium that has access to an untrusted line (see Boyle, col. 2, lines 46-65), the secure network comprising:

a. a network security controller for enabling a security officer to generate at least one user profile for each user and for sending at least one user profile to security devices connected to the network medium, each user profile defining at least one destination which the user is authorized to access through discretionary access control and mandatory access control security mechanisms, wherein a plurality of user profiles define virtual private networks of communication comprising subsets of host computers (see Boyle, col. 3, lines 30-42; col. 4, lines 27-30 and 45-53; col. 5, 33-65, especially lines 50-52; col. 6, lines 15-32; col. 8, lines 51-62, especially line 59; col. 9, lines 38-46; col. 10, lines 34-42; Figure 1 and related text); and

b. security devices connected to the network medium for receiving the user profiles generated at the network security controller and for implementing security mechanisms associated with the user profiles, each security device associated with one host computer, each security device having an authorization device for authorizing users at the associated host computer, the security device permitting the authorized user, via the associated host computer, to select a

user's profile associated with the user and for restricting access of the host computer to the at least one destination defined in the selected user's profile (see Boyle col. 5, lines 1-8; col. 7, line 46-col. 8, line 21, especially lines 47 and 51-52; col. 10, lines 31-42; Figures 1, 4A-F, and 6A).

The aforementioned covers claim 25.

As per claim 26, Boyle discloses that the at least one destination comprises at least one other host computer of the network or the untrusted line (see Boyle, Figure 2, 'Bridge (SNIU)' and 'Gateway (SNIU)'; col. 5, lines 50-53; col. 6, lines 15-20).

As per claim 27, Boyle discloses that the security devices, when implementing security mechanisms, allows the host computer to connect to a trusted destination (see Boyle, col. 10, lines 30-59).

As per claim 31, Boyle discloses that a user is prevented from simultaneously connecting to destinations having different security levels (see Boyle, col. 6, lines 15-19).

As per claim 36, Boyle discloses that the destination in a user's profile correspond to a level of security granted to the user (see Boyle, col. 4, lines 60-65; col. 6, lines 15-19; col. 9, lines 38-46).

As per claim 37, Boyle discloses that the security devices are integrated with the associated host computer (see Boyle, col. 11, lines 24-26).

As per claims 38-40, 44, and 49, they are method claims corresponding to claims 25-27, 31, and 36 and they do not teach or define above the information claimed in claims 25-27, 31, and 36. Therefore, claims 38-40, 44, and 49 are rejected as being anticipated by Boyle for the same reasons set forth in the rejections of claims 25-27, 31, and 36.

As per claim 50, Boyle discloses a secure network as outlined above in the claim 25 rejection under 102(b). In addition, the secure network is multi-level (see Boyle, Abstract) and Boyle discloses an embodiment of the invention wherein the security devices operate at a network layer (see Boyle, Figure 2, 'Gateway (SNIU)' and 'Bridge (SNIU)' and related text).

As per claim 51, Boyle discloses that the network security controller audits events (see Boyle, col. 10, lines 39-42).

As per claim 53, it is an apparatus claim corresponding to claims 39 and 50 and it does not teach or define above the information claimed in claims 39 and 50. Therefore, claim 53 is rejected as being anticipated by Boyle for the same reasons set forth in the rejections of claims 39 and 50.

As per claim 60, Boyle discloses a method for controlling a sending computer to transmit information to a receiving computer over a computer network as outlined above in the claim 25 rejection under 35 U.S.C. 103(a). In addition, Boyle discloses an embodiment of the invention wherein the security devices are implemented for internetwork connections (routing determination), and hence the security mechanisms to determine whether communication is authorized are implemented at a network layer of ISO protocol hierarchy (see Figure 2, 'Gateway (SINU)' and 'Bridge (SINU)' and related text). Furthermore, if the receiving computer is not in a transmit list and/or is not consistent with a transmit window through discretionary access control and mandatory access control, the transmission of information is terminated, otherwise the security device encrypts the information and transmits the encrypted information to the security device of the receiving computer over the computer network (see Boyle, col. 10, line 30-col. 11, line 2; col. 5, lines 33-65; col. 7, lines 43-67).

As per claims 61-64, they are method claims corresponding to claims 25, 51, and 60 and they do not teach or define above the information claimed in claims 25, 51, and 60. Therefore, claims 61-64 are rejected as being anticipated by Boyle for the same reasons set forth in the rejections of claims 25, 51, and 60.

As per claim 65, Boyle discloses a method as outlined above in the claim 60 rejection under 35 U.S.C. 103(a). In addition, Boyle discloses an embodiment of the

invention wherein the security device is a software implementation incorporated within one or more of the sending and receiving computers (see Boyle, col. 11, lines 21-32).

As per claims 69, 71, 72, and 74, they are method claims corresponding to claims 31, 60-65 and they do not teach or define above the information claimed in claims 31, 60-65. Therefore, claims 69, 71, 72, and 74 are rejected as being anticipated by Boyle for the same reasons set forth in the rejections of claims 31, 60-65.

As per claims 76-78, they are method claims corresponding to claims 60-64 and they do not teach or define above the information claimed in claims 60-64. Therefore, claims 76-78 are rejected as being anticipated by Boyle for the same reasons set forth in the rejections of claims 60-64.

As per claims 79, 81, and 83, they are method claims corresponding to claims 31, 60-65 and they do not teach or define above the information claimed in claims 31, 60-65. Therefore, claims 79, 81, and 83 are rejected as being anticipated by Boyle for the same reasons set forth in the rejections of claims 31, 60-65.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 28-30, 41-43, 52, 54, 66-68, 73, 75, 82 and 84 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boyle in view of Holden et al. U.S. Patent No. 5,828,832 (hereinafter Holden). As per claim 28, Boyle discloses a secure network as outlined above in the claim 25 rejection under 35 U.S.C. 102(b). Boyle does not expressly disclose alternative implementations of the invention wherein the host computer connects to an untrusted destination. Holden discloses a mixed enclave operation in a computer network with multi-level network security wherein the security device is configured to exploit this flexibility of mixed enclave operations (see Holden, col. 10, lines 59-60). One configuration disclosed by Holden, enables a host computer to connect to an untrusted destination wherein the security device does not implement security mechanisms (see Holden, col. 10, lines 64-67). It would be obvious to one of ordinary skill in the art at the time the invention was made to apply the teaching of Holden to the invention of Boyle. Motivation for such an implementation would enable a greater degree of flexibility with secure network host composition in the invention disclosed by Boyle, since this would allow secure hosts to communicate with unsecured hosts and still offer some protection as disclosed by Holden (see Holden, col. 11, lines 2-5).

As per claim 29, Boyle discloses a secure network as outlined above in the claim 28 rejection under 35 U.S.C. 103(a). In addition, the untrusted line comprises the Internet (see Boyle, Figure 1 as modified by Holden, Figure 1, Reference No. 36).

As per claim 30, Boyle discloses a secure network as outlined above in the claim 28 rejection under 35 U.S.C. 103(a). In addition, Holden discloses an implementation of the invention wherein a user cannot simultaneously communicate with a trusted destination and an untrusted destination (see Holden, col. 10, lines 60-63).

As per claims 41-43, they are method claims corresponding to claims 28-30 and they do not teach or define above the information claimed in claims 28-30. Therefore, claims 41-43 are rejected under Boyle in view of Holden for the same reasons set forth in the rejections of claims 28-30.

As per claim 52, it is an apparatus claim corresponding to claims 43 and 50 and it does not teach or define above the information claimed in claims 43 and 50. Therefore, claim 52 is rejected under Boyle in view of Holden for the same reasons set forth in the rejections of claims 43 and 50.

As per claim 54, Boyle covers a secure network as disclosed above in the claim 30 rejection under 35 U.S.C. 103(a). In addition, data storage devices for temporarily storing data provided by a host computer are inherent features in data processing devices that have the functions outlined by Boyle (see Boyle, col. 7, lines 43-56). Furthermore, Boyle discloses a means for transferring data out of the memory space

while making the transferred data inaccessible to the host computer (see Boyle, Figures 3A-C; col. 2, lines 46-54; col. 3, lines 3-12; col. 4, lines 40-44).

As per claims 66-68, they are method claims corresponding to claims 29-31 and 63 and they do not teach or define above the information claimed in claims 29-31 and 63. Therefore, claims 66-68 are rejected under Boyle in view of Holden for the same reasons set forth in the rejections of claims 29-31 and 63.

As per claims 73 and 75, they are method claims corresponding to claims 66, 68, and 69 and they do not teach or define above the information claimed in claims 66, 68, and 69. Therefore, claims 73 and 75 are rejected under Boyle in view of Holden for the same reasons set forth in the rejections of claims 66, 68, and 69.

As per claims 82 and 84, they are method claims corresponding to claims 66, 68, and 79 and they do not teach or define above the information claimed in claims 66, 68, and 79. Therefore, claims 82 and 84 are rejected under Boyle in view of Holden for the same reasons set forth in the rejections of claims 66, 68, and 79.

Claims 34, 47, 59, 70, and 80 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boyle. As per claim 34, Boyle discloses a secure network as outlined above in the claim 25 rejection under 35 U.S.C. 102(b). Although Boyle discloses that the network security measures of the invention are implemented at the session layer,

Boyle also teaches that end-to-end encryption devices conventionally operate at the network layer. Moreover, the invention disclosed by Boyle implements a sealer for encryption and decryption of data for secure transmission and integrity checks (see Boyle, Figure 4A, 'Sealer' and related text). It would be obvious to one of ordinary skill in the art at the time the invention was made to implement security at a network layer of protocol hierarchy. Motivation for such an implementation would enable the invention disclosed by Boyle to provide security services at the network layer and hence provide secure services without having to process the data at higher layers of the hierarchy.

As per claim 47, it is a method claim corresponding to claims 34 and 38 and it does not teach or define above the information claimed in claims 34 and 38. Therefore, claim 47 is rejected under Boyle for the same reasons set forth in the rejections of claims 34 and 38.

As per claim 59, Boyle covers a secure network as outlined above in the claim 25 rejection under 35 U.S.C. 102(b). In addition, Boyle discloses a means to update access control information by the network security controller but does not specify updating user profiles at the network security controller (see Boyle, col. 3, lines 37-39; col. 10, lines 35-37). However, as mentioned above, Boyle does disclose that the secure network is divided into two roles: the security devices implement access control based on policies that include discretionary rules, and the network security controller manages configuration management and security administration for the secure network

(see Boyle, col. 4, lines 27-30, 45-49; col. 5, lines 1-7). Furthermore, Boyle teaches that discretionary access rules are based on user identity (see Boyle, col. 5, lines 40-45). Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the network covered by Boyle to further comprise the steps of changing user profiles at the network security controller and updating available user profiles at a security device. Motivation for such an implementation would enable the method to perform updates to user profiles at the controller for centralized management of access control of all devices in the secure network.

As per claim 70, it is a method claim corresponding to claims 59 and 69 and it does not teach or define above the information claimed in claims 59 and 69. Therefore, claim 70 is rejected under Boyle for the same reasons set forth in the rejections of claims 59 and 69.

As per claim 80, it is a method claim corresponding to claims 70 and 79 and it does not teach or define above the information claimed in claims 70 and 79. Therefore, claim 80 is rejected under Boyle for the same reasons set forth in the rejections of claims 70 and 79.

Claims 32 and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boyle in view of Stallings Cryptography and Network Security 2nd Edition (hereinafter Stallings). As per claim 32, Boyle discloses a secure network as outlined

above in the claim 25 rejection under 35 U.S.C. 102(b). Boyle is silent on the matter of a user only selecting one profile during a given connection establishment. However, the feature of mapping a user to a single profile at a given time is equivalent to the well-implemented feature of a user securely logging into an account. For example, Stallings teaches how users are authenticated once per session in a Kerberos authentication service (see Stallings, Figure 11.1). By enforcing a policy of mapping a single user to a single profile, user identification and accountability can be more readily enforced. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the invention disclosed by Boyle to only allow a user to select one profile at a time. Motivation for such an implementation would enforce more stringent network connection accountability.

As per claim 45, it is a method claim corresponding to claims 32 and 38 and it does not teach or define above the information claimed in claims 32 and 38. Therefore, claim 45 is rejected under Boyle in view of Stallings for the same reasons set forth in the rejections of claims 34 and 38.

Claims 35 and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boyle in view of McNair U.S. Patent No. 5,276,444 (hereinafter McNair). As per claim 35, Boyle discloses a secure network as outlined above in the claim 25 rejection under 35 U.S.C. 102(b). Boyle is silent on the matter of at least one user profile having only one destination. However, as taught by McNair, mapping a user profile to a

plurality of destinations is an undesirable authentication feature: when a user profile that corresponds to a plurality of destinations is compromised, the plurality of destinations is compromised (see McNair, col. 1, lines 25-45). Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to establish only one destination to a user profile in the invention disclosed by Boyle. Motivation for such an implementation would enable the invention by Boyle to restrict the extent of a breach in security if a profile becomes compromised as taught by McNair.

As per claim 48, it is a method claim corresponding to claims 35 and 38 and it does not teach or define above the information claimed in claims 35 and 38. Therefore, claim 48 is rejected under Boyle in view of McNair for the same reasons set forth in the rejection of claim 35 and 38.

Claims 55-58 are rejected under 35 U.S.C. 103(a) as being unpatentable over Holden et al. U.S. Patent No. 5,802,178. As per claim 56, Holden et al. (US 5,802,178) discloses a security device for a multi-level secure network having a plurality of host computers accessible to users and connected to a computer network medium, the security device connectable between at least one host computer bus and the network medium (see Holden et al. (US 5,802,178), Abstract), the security device comprising:

a. a local bus, a local RAM, and a local processor (see Holden et al. (US 5,802,178), Figure 3, Reference Nos. 90, 82, 88 and related text, especially col. 7, lines 4-10 and 19-34);

b. a network interface for connecting the local bus to the computer network medium and including a network processing means for transferring information between the local RAM and the network medium (see Holden et al. (US 5,802,178), Figure 3, Reference Nos. 84, 90 and Figure 4, 'Hardware SNIU' and related text);

c. a communication separation means for connecting between the local bus and the host bus and for preventing direct pass-through of information between the host bus and the local bus and for preventing direct access between the host bus and the local RAM, the communication separation means including a memory device for storing information provided over the host bus in a memory space, a first port interconnecting the host bus and the memory device, and a second port interconnecting the local bus and the memory device, the information transferable from the memory space to the local bus while making the transferred information inaccessible to the host bus (see Holden et al. (US 5,802,178), Figure 3, 'Trusted Hardware', 'Shared Memory' and Figure 4, 'Hardware SNIU'; col. 3, lines 6-18; col. 4, lines 7-9 and 27-28; col. 7, lines 1-34, and 60-64; col. 8, lines 32-37;

d. wherein the local processor processes information to be transferred between the host bus and the network medium in accordance with a predetermined security policy to determine whether communication between a host computer and the network medium is authorized, the local processor including means for accessing host bus information from the memory space and

transferring the information to the local bus (see Holden et al. (US 5,802,178), col. 5, lines 32-39; col. 7, lines 4-59; Figure 3, Reference Nos. 82, 88, and 90; Figure 4, Reference No 54 and related text).

Although Holden et al. (US 5,802,178) discloses that the network security measures of the invention are implemented at the session layer (see Holden et al. (US 5,802,178), col. 3, line 67-col. 4, line 2), Holden et al. (US 5,802,178) also teaches that end-to-end encryption devices conventionally operate at the network layer. Moreover, the invention implements a Fortezza card for serivces that include encryption and decryption of data (see Boyle, Figure 4, Reference No. 56 and related text). It would be obvious to one of ordinary skill in the art at the time the invention was made to implement security at a network layer of protocol hierarchy. Motivation for such an implementation would enable the invention disclosed by Boyle to provide security services at the network layer and hence provide secure services without having to process the data at higher layers of the hierarchy. The aforementioned covers claim 56.

As per claim 57, Holden et al. (US 5,802,178) discloses a security device as outlined above in the claim 56 rejection under 35 U.S.C. 103(a). In addition, the local processor processes the host bus information in accordance with the predetermined security policy, transfers the processed host bus information to the local RAM for access by the network processing means, accesses network medium information placed in the local RAM by the network processing means, processes the network medium information in accordance with the security policy, and transfers the processed

network medium information to the communication separation means for access by the host bus (see Holden et al. (US 5,802,178), Figure 3, Reference Nos. 82, 88, and 90; Figure 4, 'Hardware SNIU' and related text; col. 7, lines 4-34; col. 5, lines 33-64).

As per claims 55 and 58, they are apparatus claims corresponding to claims 56 and 57 and they do not teach or define above the information claimed in claims 56 and 57. Therefore, claims 55 and 58 are rejected under Holden et al. (US 5,802,178) for the same reasons set forth in the rejections of claims 56 and 57.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Holden et al. U.S. Patent No. 5,802,178.

Holden et al. U.S. Patent No. 5,832,228.

Boyle et al. U.S. Patent No. 5,872,847.

Willens U.S. Patent No. 5,889,958.

Boyle et al. U.S. Patent No. 5,940,591.

Nickles U.S. Patent No. 6,134,591.

Boyle et al. U.S. Patent No. 6,212,636.

Williams U.S. Patent No. 6,304,973.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (703) 305-8289. The examiner can normally be reached on M-F 9:00 A.M. to 6:00 P.M. except every other Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Jung W Kim
Examiner
Art Unit 2132

Jk
December 10, 2003

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100